Privacy Impact Assessment for the VA IT System called:

MuleSoft Gov Cloud -Enterprise (MuleSoft -E)

Veterans Affairs Office of Information and Technology Development, Security, and Operations Digital Transformation Center

Veterans Affairs Central Office

eMASS ID #1097

Date PIA submitted for review:

01/15/2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	OITPrivacy@va.gov tonya.facemire@va.gov	(202) 632-8423
Information System Security Officer (ISSO)	Andrew Longtine	Andrew.longtine@va.gov	320-333-2017
Information System Owner	Jerry Abernathy	Jerry.Abernathy@va.gov	202-459-3509

Abstract

The abstract provides the simplest explanation for "what does the system do for VA?".

MuleSoft GovCloud – Enterprise (MuleSoft-e) is a hybrid platform for designing, developing, and managing APIs and integrations. Uniquely built as a single solution, it includes integration Platform as a Service (iPaaS) functionality which provides users with enterprise messaging, advanced user and role-based management, services/tools for providing API and integration analytics and management, API design and publishing tools, and the ability to share and collaborate on API specifications, code snippets and templates of best practices. MuleSoft ESB at VA is used to retrieve real time information between Salesforce and VA systems via API. MuleSoft-e is a Platform as a Service (PaaS) and is considered middleware.

Overview

The overview is the most important section of the Privacy Impact Assessment (PIA). A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

A. *What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*

MuleSoft GovCloud – Enterprise (MuleSoft-e) is a hybrid platform for designing, developing, and managing APIs and integrations. Uniquely built as a single solution, it includes integration Platform as a Service (iPaaS) functionality allowing users to receive data from one or more independent systems. MuleSoft Cloud Enterprise (MuleSoft-e) owned in collaboration between Veterans Affairs Office of Information and Technology (OI&T), Development, Security, and Operations (DevSecOps), Digital Transformation Center (DTC), and Veterans Affairs Central Office (VACO).

B. *Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.*

MuleSoft Cloud Enterprise (MuleSoft-e) is a VA Controlled / non-VA Owned and Operated. MuleSoft-e is a Platform-as-a-Service (PaaS) development environment that supports Veterans Affairs Central Office (VACO). VA MuleSoft-e is an enterprise-wide system.VA MuleSoft-e System Administrators, and personnel delegated by the administrator, have access permissions that allow the user to access the platform Setup. The platform setup contains options to customize MuleSoft-e and build, deploy, and manage integrations.

2. Information Collection and Sharing

C. Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?

MuleSoft as a middleware; it does not provide access to end users but allows information to pass between VA systems. Performance metrics are only on the business units data processing between the VA systems and not data storage. VA MuleSoft-e processes from Veterans or dependents, VA employees, and VA contractors. Program officials have identified the minimum PII data elements required to be processed by MuleSoft-e system. The data elements will be processed from VA System using automation via application programming interfaces (APIs) to support specific VA business process and the subset of the PII VA is authorized to collect.

Check if Applicable	Demographic of individuals
☒	Veterans or Dependents
☒	VA Employees
☐	Clinical Trainees
☒	VA Contractors
☒	Members of the Public/Individuals
☐	Volunteers

D. What is a general description of the information in the IT system and the purpose for collecting this information?

In accordance with the VA Office of Information and Technology (OIT) guidance, MuleSoft-e is deployed in AWS being managed by VACO. MuleSoft-e provides critical integration services back into the VA legacy systems to provide the interface for modules to work directly with the VA Systems.

E. What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.

MuleSoft-e consists of several key components called Application Programming Interface (APIs). Each API will be evaluated to determine if any data elements of that module processes PII.

F. Are the modules/subsystems only applicable if information is shared?

MuleSoft-e is an enterprise-wide system. The primary site will be the Amazon Web Services (AWS) GovCloud (West) region. The security controls protecting the PII data processed within MuleSoft-e are documented in the approved MuleSoft-e Authority To Operate (ATO). The specific security controls leveraged by MuleSoft-e, in addition to a detailed description of the MuleSoft-e security boundaries, are documented in the System Security Plan (SSP).

G. Is the system operated in more than one site to include primary and secondary site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?

MuleSoft -e infrastructure is not managed by the local facility and is hosted on Amazon Web Services GovCloud (US). The Enterprise manages all the critical data centers. Alternate Data Processing processes/activities will vary depending on the systems affected. It also includes the necessary storage space to backup duplicate copies of information and data.

3. Legal Authority and System of Record Notices (SORN)

H. What is the citation of the legal authority?

Legal Authority to operate is as follows:

- MuleSoft FedRAMP Package authorized since March 6, 2023 and valid through March 5, 2026.
- To obtain package, agency employees and contractors must complete OMB MAX registration form. The package name is MuleSoft Government Cloud FedRAMP and package ID is FR1818161169 Authority to Operate (ATO) for MuleSoft-e was authorized on March 6, 2023 and valid through March 5, 2026

I. What is the SORN?

MuleSoft -e is not a system of records and only captures meta data. There is no SORN applicable to the system, as information about individuals is not retrieved from the IT system by a unique identifier.

J. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.

This is not applicable, as a SORN is not required for this IT system.

4. System Changes

J. Will the business processes change due to the information collection and sharing?

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

K. Will the technology changes impact information collection and sharing?

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 Information collected, used, disseminated, created, or maintained in the system.

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority to Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- ☒ Name
- ☐ **Full** Social Security Number
- ☐ **Partial** Social Security Number
- ☐ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a Different Individual)
- ☒ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account Numbers
- ☐ Certificate/License Numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender/Sex
- ☒ Integrated Control Number (ICN)
- ☒ Military History/Service Connection

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

☐ Next of Kin
☐ Date of Death
☐ Business Email Address
☐ Electronic Data Interchange Personal Identifier (EDIPI)
☐ Other Data Elements (List Below)

Other PII/PHI data elements: <<Add Additional Information Collected but Not Listed Above Here (For Example, Biometrics)>>

1.2 List the sources of the information in the system

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Sources of data include two-way integration from internal VA systems to include Salesforce-e, Austin Information Technology Center (AITC) Infrastructure Operations (IO), Financial Services Center (FSC), Digital Transformation Center (DTC) Integration Platform (DIP), Prosthetics Order Vendor Interface and Delivery Tracking Solution (POVIDTS), Beneficiary Travel Self Service System Assessing (BTSSS), VA Microsoft Dynamics (MS Dyn 360), and VA Salesforce Data Center (SFDC), Medical Disability Examination Office (Salesforce), Qualtrics/ Office of General Counsel (BOX), Office of Strategic Sourcing (Salesforce), and Summit Data Platform.

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

MuleSoft-e is used to exchange information and provide data between separate IT systems. In addition, it provides protocol transformation capabilities between applications for user enhancement purposes or to provide system monitoring metrics for auditing and performance.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

MuleSoft-e generates reports on the performance and metrics of its underlying system. These reports are used to monitor and audit the system to ensure efficient data flow.

1.3 Methods of information collection

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

MuleSoft-e does not originate the collection of data. Sources of data include two-way integration from internal VA systems to include to include Salesforce-e, Austin Information Technology Center (AITC) Infrastructure Operations (IO), Financial Services Center (FSC), Digital Transformation Center (DTC) Integration Platform (DIP), Prosthetics Order Vendor Interface and Delivery Tracking Solution (POVIDTS), Beneficiary Travel Self Service System Assessing (BTSSS), VA Microsoft Dynamics (MS Dyn 360), and VA Salesforce Data Center (SFDC), Medical Disability Examination Office (Salesforce), Qualtrics/ Office of General Counsel (BOX), Office of Strategic Sourcing (Salesforce), and Summit Data Platform.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

MuleSoft-e PII/PHI is not collected on a form and hence not subjected to Paperwork Reduction Act. MuleSoft only allows data transmission and receival.

1.4 Information checks for accuracy, and how often will it be checked.

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

Personally Identifiable Information is processed in the system and not maintained or retrievable. It is used in transport as a Platform as a Service (PaaS) middleware.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

MuleSoft-e does not inherently validate data accuracy by accessing commercial aggregator of information. Its primary function as middleware is to enable data integration and monitor its systems performance and stability.

1.5 Identify the specific legal authorities, arrangements, and agreements that defined the collection of information.

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

The legal authorities that authorize MuleSoft-e to process PII are as follows:

- 5 U.S.C. 552, "Freedom of Information Act," c. 1967

- 5 U.S.C. 552a, "Privacy Act," c. 1974
- 18 U.S.C. 1030 (a) (3), "Fraud and related activity in connection with computers."
- 38 U.S.C. 218, "Security and law enforcement on property under the jurisdiction of the Veterans Administration"
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems
- Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)
- Federal Information Security Management Act (FISMA) of 2002
- OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E Government Act of 2002
- Executive Order 13103, Computer Software Privacy
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- FIPS 201-1, Personal Identity Verification of Federal Employees and Contractors
- FIPS 140-2, Security Requirements for Cryptographic Module

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

Principle of Purpose Specification: The collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.

Principle of Data Quality and Integrity: VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.
This is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: MuleSoft-e has been categorized as moderate in which compromise could result in serious but manageable consequences to the affected parties. These can include financial harm, damage to reputation, or erosion of trust, but are not expected to cause life altering or irreparable harm. Risk that if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, or financial harm may result for the individuals affected.

Mitigation: The system employs a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. Security controls are in place as well as access control, awareness and training, audit, and accountability, certification, and accreditation. The system operates under guidance provided in the National Institute of Standards and Technology (NIST) Special Publication 800-37 and specific VA directives.

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system that will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

MuleSoft-e is a Platform as a Service (PaaS) middleware that processes data. Data is not retained or retrievable. The types of data include Veteran Internal Control Number (ICN), Full Name, Address, Military History, and Service Connection.

PII/PHI Data Element	Internal Use	External Use
Name	Internal APIs on systems to include • Austin Information Technology Center (AITC) Infrastructure Operations (IO) • Financial Services Center • Digital Transformation Center (DTC) Integration Platform • Prosthetics Order Vendor Interface and Delivery Tracking Solution (Salesforce) • Veterans Engagement Reporting Application (Salesforce) • Medical Disability Examination Office (Salesforce) • Qualtrics/ Office of General Counsel (BOX) • Office of Strategic Sourcing (Salesforce)	Not used
Address	Internal APIs on systems to include • Prosthetics Order Vendor Interface and Delivery Tracking Solution (Salesforce) • Medical Disability Examination Office (Salesforce)	Not used
Veteran Internal Control Number	Internal APIs on systems to include • Caregiver Record Management Application (Salesforce) • Beneficiary Travel Self Service System Assessing	Not used

	• VA Microsoft Dynamics 365 • VA Salesforce Data Center • Medical Disability Examination Office (Salesforce) • Summit Data Platform	
Financial Account Number	Internal APIs on systems to include • Prosthetics Order Vendor Interface and Delivery Tracking Solution (Salesforce)	Not used
Phone Number	Internal APIs on systems to include • Veterans Engagement Reporting Application (Salesforce) • Qualtrics/ Office of General Counsel (BOX)	Not used
Personal Email Address	Internal APIs on systems to include • Prosthetics Order Vendor Interface and Delivery Tracking Solution (Salesforce) • Veterans Engagement Reporting Application (Salesforce)	Not used
Military History/ Service connection	Internal APIs on systems to include • Medical Disability Examination Office (Salesforce)	Not used

2.2 Describe the types of tools used to analyze data and what type of data may be produced.
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

MuleSoft-e acts as Platform as a Service (PaaS). Data processed is not a permanent repository and is updated in internal VA source systems. Analysis will be conducted on source system.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

MuleSoft-e acts as a middleware and does not create or make available new or previously unutilized information about an individual.

2.3 How the information in the system is secured.

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

MuleSoft-e is a PaaS and processes data. Data is not retained and not at rest. Social Security Numbers are not processed. Remaining data elements are protected with FIPS 140-2 encryption. Supervisory assignment of functional categories restricting employee access to systems information.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

Social Security Numbers are not processed.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?

MuleSoft-e is a PaaS and processes data. Data is not retained and not at rest. Remaining data elements are protected with FIPS 140-2 encryption. Supervisory assignment of functional categories restricting employee access to systems information.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

All persons granted access to VA systems are granted that access based on their position, duties, and a job related need to know. All individuals granted access to this system are required to have extensive training prior to receiving access and are required to recertify annually that he/she understands VA's commitment to continuous readiness in information security.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

All information processed with this system is handled in accordance with policies and procedures related to information security determined by the VA. All documentation is within eMASS and updated continuously as changes occur.

2.4c Does access require manager approval?

All persons granted access to VA systems are granted that access based on their role.

2.4d Is access to the PII being monitored, tracked, or recorded?

Access to PII is monitored and tracked in accordance with VA mandates as outlined within eMASS and relevant security controls.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

Responsibility for PII identified in eMASS is assigned to the ISSO, ISO, and System Steward.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

MuleSoft-e is an integration Platform as a Service(iPaaS). Information is passed through but not retained.

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.

MuleSoft-e is an integration Platform as a Service(iPaaS). Information is passed through but not retained.

3.3 The retention schedule approved by the VA records office and the National Archives and Records Administration (NARA).

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. Please work with the system VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

MuleSoft-e is an integration Platform as a Service(iPaaS). Information is passed through but not retained.

3.3b Please indicate each records retention schedule, series, and disposition authority?

SORN is not applicable for the system as information are not retained by MuleSoft-e.

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated, or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

MuleSoft-e is an integration Platform as a Service(iPaaS). Information is passed through but not retained.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training, and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

The use of PII during research, testing, and training is reduced when possible, to minimize risk. PII is not used in research. PII is minimally used in testing and training when de-identifier data is not able to be used due to system constraints. Instances of testing and training that contain PII, adherence to VA Handbook 6500 is followed.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System Privacy Officer (PO) to complete all Privacy Risk questions inside the document in this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

Principle of Minimization: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

Principle of Data Quality and Integrity: The PIA should describe policies and procedures for how PII that is no longer relevant and necessary is purged.
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: PII is processed but not retained or retrievable.

Mitigation: The privacy risk is mitigated by the security controls in place for MuleSoft-e. VA Handbook 6500 and 6301 as well as NIST 800-53 moderate impact defined set of controls are followed.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

PII Mapping of Components

4.1a MuleSoft -e consists of zero key components (servers/ databases/ instances/ applications/ software/ application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by MuleSoft -e and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9a in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
N/A	N/A	N/A	N/A	N/A	N/A

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Caregiver Record Management Application (Salesforce)	Internal VA system integration	Veteran Internal Control Number (ICN), Veteran Name	Two-way SSL integration
Austin Information Technology Center (AITC) Infrastructure Operations (IO)	Internal VA system integration	Veteran Name	Two-way SSL integration
Financial Services Center	Internal VA system integration	Veteran Name	Two-way SSL integration
Digital Transformation Center (DTC) Integration Platform	Internal VA system integration	Veteran Name	Two-way SSL integration
Prosthetics Order Vendor Interface and Delivery Tracking Solution (Salesforce)	Internal VA system integration	Veterans - Name, Address, Financial Account information. VA Employee and VA Contractor Name	Two-way SSL integration
Beneficiary Travel Self Service System Assessing	Internal VA system integration	Veteran Internal Control Number (ICN)	Two-way SSL integration
VA Microsoft Dynamics 365	Internal VA system integration	Veteran Internal Control Number (ICN)	Two-way SSL integration
VA Salesforce Data Center	Internal VA system integration	Veteran Internal Control Number (ICN)	Two-way SSL integration
Veterans Engagement Reporting Application (Salesforce) (graph.microsoft.com.va.gov/VA notify API)	Internal VA system integration	Veteran - Name, Phone Number and E-mail Address	Two-way SSL integration
Medical Disability Examination Office (Salesforce)	Internal VA system integration	Veteran Name, Veteran ICN, Address, Military History/ Service Connection	Two-way SSL integration
Qualtrics/ Office of General Counsel (BOX)	Internal VA system integration	Name, Personnel E-mail, Personnel Phone Number	Two-way SSL integration

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
Office of Strategic Sourcing (Salesforce)	Internal VA system integration	Veteran Name	Two-way SSL integration
Summit Data Platform	Internal VA system integration	Veteran Internal Control Number (ICN)	Two-way SSL integration

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions in this section.).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: There is a risk that information may be shared with unauthorized VA Program, or individual.

Mitigation: All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. MuleSoft-e adheres to all information security requirements instituted by the VA Office of Information Technology (OIT). Information is shared in accordance with VA Handbook 6500. Windows and Unix access controls are provided by VA's Infrastructure Operations (IO), along with the following security controls: Audit and Accountability, Awareness Training, Security Assessment and Authorization, Incident Response, Personnel Security, and Identification and Authentication. The safeguards implemented to ensure data is not sent to the wrong VA organization are employee security privacy training and awareness and required reporting of suspicious activity. Use of Two-Factor Authentication (2FA), access for need to know basis, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: MuleSoft -e does not have any external integrations and hence has limited risk of exposure of information.

Mitigation: MuleSoft -e does not have any external integrations. Additionally, safeguards are implemented to ensure data is not sent to the wrong VA organization are employee security privacy training and awareness and required reporting of suspicious activity. Use of Two-Factor Authentication (2FA), access for need to know basis, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

MuleSoft-e is a Platform as a Service (PaaS) and is considered middleware. Data is not collected but passed through the system. A System of Records Notice (SORN) is not required.

6.1b If notice was not provided, explain why.

Notice is not provided, since MuleSoft -e is a middleware.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

Notice is not provided, since MuleSoft -e is a middleware.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

MuleSoft-e is a Platform as a Service (PaaS) and is considered middleware. Data is not collected but passed through the system.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

MuleSoft-e is a Platform as a Service (PaaS) and is considered middleware. Data is not collected but passed through the system.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your Privacy Officer (PO) to complete all Privacy Risk questions inside the document this section).

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: This is referring to sufficient notice provided to the individual.

Principle of Use Limitation: The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must ensure that information is used only for the purpose articulated in the notice.
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.

Follow the format below:

Privacy Risk: MuleSoft-e is a Platform as a Service (PaaS) and is considered middleware. Data is not collected but passed through the system. Privacy information may be collected prior to providing written notice.

Mitigation: The VA mitigates this risk by providing Veterans and other beneficiaries with multiple forms of notice of information collection, retention and processing.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 The procedures that allow individuals to gain access to their information.

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

MuleSoft-e is a Platform as a Service (PaaS) and is considered middleware. Data is not collected but passed through the system.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?

MuleSoft-e is a Platform as a Service (PaaS) and is considered middleware. Data is not collected but passed through the system.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?

MuleSoft-e is a Platform as a Service (PaaS) and is considered middleware. Data is not collected but passed through the system.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

MuleSoft-e is a Platform as a Service (PaaS) and is considered middleware. Data is not collected but passed through the system.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

MuleSoft-e is a Platform as a Service (PaaS) and is considered middleware. Data is not collected but passed through the system.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

MuleSoft-e is a Platform as a Service (PaaS) and is considered middleware. Data is not collected but passed through the system.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

Principle of Individual Participation: If access and/or correction is denied, then is the individual must be provided notice as to why the denial was made and how to challenge such a denial.

Principle of Individual Participation: The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their knowledge.
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: MuleSoft-e is a Platform as a Service (PaaS) and is considered middleware. Data is not collected but passed through the system. There is a risk individuals may attempt to access information processed about them by the VA Office.

Mitigation: By publishing this PIA, the VA makes the public aware of the unique status of information processed on this platform. Furthermore, this document provides the point of contacts for members of the public who have questions or concerns.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be documented.

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?

All individuals are subject to a background investigation before system access is granted. All individuals with system access are required to complete the VA Privacy and Information Security Awareness and Rules of Behavior training annually.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

There have not been individual users from other agencies that have access. All users are subject to a background investigation before system access is granted. All individuals with system access are required to complete the VA Privacy and Information Security Awareness and Rules of Behavior training annually.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

MuleSoft-e users have access privileges identified by their supervisors as needed to perform their assigned duties. The Requesting Official is responsible for ensuring that the user's access is restricted to only those applications and functions that are required for the user to perform their assigned duties and that separation of duty has been applied as appropriate.

8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.

How frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

8.2a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

Yes, VA contract employee access is verified through the Contracting Officer's Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system. Contractor access is reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information Security Officer, Privacy Officer, Contracting Officer Representative, Procurement Requestor/Program Manager and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

8.2b. Will VA contractors have access to the system and the PII?

Yes.

8.2c. What involvement will contractors have with the design and maintenance of the system?

Contractors may have access to MuleSoft-e. All contractors sign the VA Rules of Behavior, just as VA Employees do, and they pass a Background Investigation prior to receiving access to VA Systems

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system.

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the VA Privacy and Security Awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the privacy and security awareness training.

Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information. System administrators are required to complete additional role-based training.

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If completed, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 07-November-2024
3. *The Authorization Status:* Authorization to Operate
4. *The Authorization Date:* 06-March-2023
5. *The Authorization Termination Date:* 05-March-2026
6. *The Risk Review Completion Date:* 15-Febuary-2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

8.4b If not completed or In Process, provide your ***Initial Operating Capability (IOC) date.***

N/A

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties. ***(Refer to question 1.8 of the PTA)***

MuleSoft integration Platform as a Service (iPaaS), MuleSoft is hosted in the Amazon Web Services GovCloud (US). MuleSoft-f FedRAMP environment and is authorized. MuleSoft-f (FedRAMP) was granted a full ATO on 03/06/2023 that is valid through 03/05/2026 The FIPS 199 classification is Moderate.

9.2 Does the contract with the Hosting Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.1*

of the PTA) *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Data is owned by the VA and is processed through MuleSoft based on VA guidelines. MuleSoft has the responsibility of notifying VA of actual or reasonably suspected unauthorized disclosure of VA Data by MuleSoft or those acting on its behalf. The contract number is NNG15SD27B 36C10B23F0172. Information processed is in accordance with VA policies.

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

No, the CSP will not collect ancillary data.

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Data is owned by the VA and is processed through MuleSoft based on VA guidelines. MuleSoft has the responsibility of notifying VA of actual or reasonably suspected unauthorized disclosure of VA Data by MuleSoft or those acting on its behalf. Information processed is in accordance with VA policies. The ultimate accountability for the security and privacy held by the cloud provider on VA's behalf is described in the contract # NNG15SD27B 36C10B23F0172. Department of Veterans Affairs is the owner of all data to include PII. The magnitude of potential harm to the VA privacy release data is low to moderate due to the potential of identity theft or unauthorized release of PII. An unauthorized disclosure could negatively affect the reputation of the VA and MuleSoft as well as a reduction of public trust.

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

MuleSoft-e does not use Robotics Process Automation (RPA).

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

The individuals below attest that the information provided in this Privacy Impact Assessment is true and accurate.

TONYA FACEMIRE

Digitally signed by TONYA FACEMIRE
Date: 2025.01.28 08:56:48 -05'00'

Privacy Officer, Tonya Facemire

ANDREW LONGTINE

Digitally signed by ANDREW LONGTINE
Date: 2025.01.28 11:29:20 -06'00'

Information Systems Security Officer, Andrew Longtine

JERRY ABERNATHY

Digitally signed by JERRY ABERNATHY
Date: 2025.01.29 16:21:03 -06'00'

Information Systems Owner, Jerry Abernathy

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Directive 1605.04
IB 10-163p (va.gov)